A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts
AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

No. 1999-1058-4X

OFFICE OF THE STATE AUDITOR'S REPORT ON INTERNAL CONTROLS OVER THE DEPARTMENT OF SOCIAL SERVICES' FAMILYNET SYSTEM

February 1, 1999 through November 1, 2000

OFFICIAL AUDIT REPORT
NOVEMBER 16, 2001

1999-1058-4X

TABLE OF CONTENTS

Page

INTRODUCTION 1

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY 3

AUDIT SUMMARY 8

AUDIT RESULTS 13

1. System Access Security 13

2. Security over Hardcopy Client Records 16

APPENDICES

Appendix A
Review of Physical Security and Environmental Protection at Selected DSS Offices 21

Appendix B
Summary of Selected Responses to the User Survey Questionnaire 23

INTRODUCTION

The Department of Social Services (DSS) is organized under the authority of Chapter 18B, Section 1, of the Massachusetts General Laws, as amended, and is placed within the Executive Office of Health and Human Services (EOHHS). The DSS operates from a central office in Boston and is organized into six regional offices that oversee 29 area offices throughout the Commonwealth. The DSS is comprised of a commissioner, two deputy commissioners, five assistant commissioners, a general counsel, and six directors who have overall responsibility for operational programs, such as domestic violence and family support services, family-based services, and residential/adolescent services. Six regional directors supervise operations at the regional offices. DSS is staffed by approximately 3,100 employees.

The Department of Social Services is dedicated to the long-term safety and well being of children who have been abused or neglected in a family setting. The Department's mission is to keep families together. To achieve this goal, DSS provides family-based services to assist parents in better caring for their children. For those children who are unable to remain at home because of severe abuse or neglect or who are at risk of abuse and neglect, DSS provides temporary out of home care through foster care, group care, or residential programs. These short-term measures are used to provide interim guidance and support to families until children can safely be returned home. In cases where this is not possible, DSS attempts to provide a child with an alternate long-term solution such as adoption, guardianship, or, as with older teenagers, independent living. At the end of the 2000 fiscal year, there were 72,423 clients with open cases who were receiving services. In addition to providing services to 62,147 clients, DSS provided services for foster care/residential care placements and placements in other non-referral locations such as hospitals, state agencies, and homes of relatives and family friends to 10,276 young adults and children. Further, 870 children under DSS care had their adoptions finalized during the 2000 fiscal year.

DSS relies heavily on information technology to help carry out its mission and business objectives. In March 1996, DSS signed an implementation contract with Deloitte & Touche, LLP to develop FamilyNet, a local area network (LAN)-based, custom-designed, comprehensive, integrated, automated system that would replace the Area-based Social Service Information System Technology (ASSIST), the prior mainframe-based system that had been implemented in the early 1980s. The FamilyNet system, which was developed using federal guidelines for Statewide Automated Child Welfare Information Systems (SACWIS), was implemented in February 1998.

State and federal monies were used to fund the development of FamilyNet. According to DSS, the total cost for the development and implementation of FamilyNet was approximately

$51.64 million, of which approximately $16.50 million (32%) was comprised of state funds and $35.14 million (68%) was comprised of federal funds.

According to the "request for proposal" for the implementation of FamilyNet, the system was required to address the significant limitations and deficiencies of ASSIST, "regarding its ability to support casework investigation, assessment, and service delivery." According to DSS management, ASSIST was used infrequently because staff had great difficulty accessing the system, many screens were required to enter data, and the system lacked current, reliable information. Because ASSIST's functionality did not address all critical DSS business activities, the Department also had to use several microcomputer-based programs, e.g., software used for adoption-related services.

FamilyNet was developed to properly support caseworkers in the following functions: intake and screening, investigations, assessments, case management, adoption services, and family resource services, and to help ensure system availability and meet regulatory requirements, such as those for federal reporting. In addition, FamilyNet functions were developed to include tracking and analysis of financial information; monitoring and maintenance of various service providers; providing a means to help ensure comprehensive quality assurance; providing support for supervisors regarding distribution of case assignments, case monitoring and case tracking; planning for structured services and delivery of services to clients; and providing for daily case management activities.

The DSS information technology (IT) infrastructure used to support FamilyNet and administrative applications consists of local area networks installed at the central office, and regional and area offices. The local area networks are connected to the state's wide area network (WAN). FamilyNet's database resides on the file server located at the Massachusetts Information Technology Center (MITC) operated under the aegis of the Commonwealth's Information Technology Division (ITD). Because the MITC's file server containing the FamilyNet database is part of the network that is connected to the WAN, all DSS offices can access FamilyNet data files and software.

Our Office's examination focused on a review of selected internal controls over the FamilyNet system, specifically physical security and environmental protection controls over IT resources at the central office, regional offices, and a sample of area offices; system access security; business continuity planning; and on-site storage of computer-related media. In addition, we reviewed control practices regarding security over hardcopy confidential client records and evaluated management and staff satisfaction with selected functions of the FamilyNet system.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From May 22, 2000 through November 1, 2000, we performed an audit of selected information technology (IT)-related controls at the Department of Social Services (DSS) for the period covering February 1, 1999 through November 1, 2000. The scope of our audit included a review and evaluation of system access security to the FamilyNet system and a review of access controls over the network on which the FamilyNet application resides. In addition, we examined control practices, procedures, and devices regarding physical security and environmental protection over and within the buildings housing DSS business offices, ten computer rooms and automated systems installed at the central office in Boston and at six regional and nine area offices. Further, we reviewed physical security and environmental protection over restricted areas housing confidential client records at the business offices and on-site storage for computer-related media. We examined control practices regarding the security over and destruction and removal of hardcopy confidential information regarding DSS clients. In conjunction with our audit, we reviewed formal policies and procedures promulgated by DSS regarding controls and operations with respect to the audit objectives for the areas under review.

Regarding system availability, we reviewed business continuity planning for the daily casework and administrative and financial operations processed through the FamilyNet system. With respect to the restoration of normal business functions, we reviewed the adequacy of formal policies and procedures regarding business continuity planning and the physical security and environmental protection of backup media stored on-site and off-site. In addition, we surveyed and evaluated management and staff satisfaction with selected functions of FamilyNet.

Audit Objectives

Our primary audit objective was to determine whether adequate security controls were in place and in effect to provide reasonable assurance that only authorized parties could access the FamilyNet system and IT resources and that system information is sufficiently protected against unauthorized disclosure, change, or deletion. In addition, we determined whether adequate controls had been implemented to provide reasonable assurance that only authorized users were granted access to the FamilyNet application and that unauthorized access was prevented or detected. We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to restrict access to IT resources, including confidential client records in hardcopy form, to only authorized users in order to prevent unauthorized use, damage, or loss of IT resources. A further objective was to determine whether adequate control practices were in place regarding the removal and/or disposal of hardcopy client records. In conjunction with our audit, we sought to determine whether DSS had complied with regulatory requirements, including the Code of Massachusetts Regulations (CMR) regarding security and disposal over hardcopy client records. We sought to determine whether adequate business continuity planning had been performed and whether plans were in place to restore mission-critical and essential business operations in a timely manner should the FamilyNet system be unavailable for an extended period. Further, we determined whether physical security and environmental protection regarding on-site storage areas for computer-related media were adequate. We did not review the off-site storage location. Another objective was to review and evaluate management and staff satisfaction with the FamilyNet application system.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of the automated and manual components of the FamilyNet system. Through pre-audit interviews with managers and staff, reviews of system documentation, and demonstrations of selected functions of the FamilyNet system, we obtained and recorded an understanding of the primary business functions processed through the automated system. We reviewed automated and manual functions regarding procedures used to record inquiries from the public, enter client records into FamilyNet, provide casework services, and discharge clients. We documented the significant functions and activities supported by FamilyNet, and reviewed automated functions related to operations designated as critical by DSS. We reviewed the FamilyNet system's data dictionary that is the repository of naming conventions and each data element, description, and operational function in the information system. Further, we gained an understanding of and documented electronic interfaces currently in place between FamilyNet and federal and state agencies, such as the federal Social Security Administration, Massachusetts Department of Medical Assistance, Massachusetts Department of Transitional Assistance, Massachusetts Department of Revenue, and the Office of the State Comptroller. We also reviewed and documented the electronic interface then under development with the Massachusetts Department of Youth Services.

We conducted additional pre-audit work, which included reviewing the role of the DSS central office regarding physical security and environmental protection over business offices and restricted areas housing client records at Department offices. As part of pre-audit, we reviewed relevant documents, such as the DSS internal control plan, the Executive Office for Administration and Finances' request for proposal for SACWIS, the Department's network configuration, the DSS draft data security policy, and the Records Management Manual. In addition, we interviewed DSS central office management to discuss internal controls regarding physical security and environmental protection over and within business offices, the computer room at the central office, and local area networks (LAN) installed at the central office, regional offices, and selected area offices, and on-site and off-site storage of critical computer-related backup media. Further, we performed a preliminary review of internal controls related to physical security over hardcopy client records located at DSS area offices. We reviewed procedures used to collect backup media for administrative applications such as word processing from regional and area offices for transport to MITC and, subsequently, to a vendor's off-site location. Further, we reviewed procedures used by MITC for daily backup of the FamilyNet database and transport of the computer-related media for storage at a vendor's off-site location. We did not review the controls in place at the MITC or the vendor's off-site storage location. Prior to the inception of our substantive audit work, we discussed the scope and objectives of our audit with senior management at the DSS central office.

We determined whether the DSS central office had developed and implemented written, authorized, and approved policies and procedures regarding physical security, environmental protection, system access security and security over and disposal of client records in accordance with regulatory requirements. In addition, we reviewed, associated written policies and procedures developed by regional and area offices. We reviewed the Department's documented business continuity plan and associated policies and procedures to determine whether adequate standards and guidelines were provided to assist staff in restoring business functions in a timely manner. We determined whether the documentation provided management and users sufficient standards and guidelines to describe, review, and comply with statutes, regulations and generally accepted control objectives for IT operations and security. Subsequent to the completion of our pre-audit work, we developed an audit program based upon the results of our pre-audit using benchmark Control Objectives for Information and Related Technology (CobiT). CobiT is a systematic framework of IT-related control objectives, standards, and practices used by managers, information system auditors, and users.

To determine whether physical access over IT-related resources, including computer equipment, was restricted to only authorized users and that these IT resources were adequately safeguarded from loss, theft or damage, we performed audit tests at the central office, six regional offices, and nine area offices located throughout the Commonwealth. We visited all six regional offices and nine (32%) of the 29 area offices that were chosen judgmentally for review. We reviewed physical security and environmental protection over IT-related equipment through inspection and interviews with DSS management and staff. We interviewed the administrative manager and security manager at each regional and area office that we visited. To determine whether adequate controls were in effect to prevent and detect unauthorized access to business offices housing automated systems and ten computer rooms, we inspected physical access controls, such as appropriately locked entrance and exit doors, the presence of a receptionist, burglar alarms, and whether visitor badges were being issued. We reviewed access control procedures, such as key management for entrance and exit door locks on computer rooms and other restricted areas within business offices. We reviewed incident report logs to identify security-related events, such as unauthorized entry attempts, threatening phone calls, or thefts of computer-related equipment. Further, we determined whether incident logs were reviewed and whether corrective actions had been taken to address security-related incidents.

To determine whether adequate controls were in effect to physically secure and properly dispose of confidential client records, we inspected restricted areas within business offices where confidential client records were stored. We determined whether doors to the restricted areas were locked and whether file cabinets used to store client records were secured. To determine whether only authorized DSS and contractor staff were granted access to client records, we interviewed central office management and each area office administrative manager and reviewed lists of staff and vendors authorized to access these records. We reviewed sign-out/sign-in procedures for client records at selected offices. Further, we reviewed control practices regarding the disposal of client records, including the use of shredding machines to destroy confidential documents at DSS offices. Moreover, we reviewed procedures used by DSS to transfer records to contractor shredding and disposal companies for additional shredding. We inspected trash receptacles at business offices where shredded documents were to be kept prior to disposal and we inspected trash dumpsters to determine whether they were being kept locked.

To determine whether adequate environmental protection controls were in effect to properly safeguard automated systems and hardcopy client records from loss or damage, we checked for the presence of fire alarms, fire control methods such as sprinklers and inert-gas fire suppression systems, controls to prevent power surges, such as surge protectors for automated systems, and emergency power generators and lighting. We reviewed general housekeeping procedures to determine whether only appropriate office supplies and equipment were placed in computer rooms or in the vicinity of computer-related equipment. To determine whether proper temperature and humidity controls were in place, we reviewed for the presence of appropriate dedicated air-conditioning units in business offices, computer rooms, and on-site storage areas. Further, we reviewed control procedures to prevent water damage to automated systems, client records, and computer-related backup media for on-site storage.

To determine whether DSS control practices regarding system access security adequately prevented and detected unauthorized access to automated systems, we reviewed policies and procedures regarding system access and data security, interviewed the network and database administrators, and evaluated access controls to FamilyNet network and application.

To determine whether the administration of logon ID and passwords was being properly carried out, we initially reviewed internal control documentation regarding system access security. We then reviewed the security procedures with the network administrator responsible for access to the LANs on which the FamilyNet system operates and central office management responsible for supervising FamilyNet. We reviewed the access privileges of DSS and outsourced staff authorized to access

FamilyNet. To determine whether controls in place were adequate to ensure that access privileges to the automated systems were granted only to authorized users, we reviewed and evaluated procedures for authorizing and deactivating access to FamilyNet's data files and software. We then compared a sample of individuals authorized to access the automated systems to the DSS payroll records or list of outsourced staff to determine whether all users were current employees or outsourced staff. We determined whether all employees and outsourced staff authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes. In addition, we reviewed control practices used to assign DSS and outsourced staff access to the FamilyNet application programs and data files. We observed and evaluated an actual demonstration FamilyNet's system administrator of system access control practices.

To assess business continuity efforts, we reviewed the adequacy of formal planning to resume mission-critical and essential operations should the LANs' file servers and the microcomputer systems on which FamilyNet operates be damaged or destroyed. We interviewed the senior manager in charge of FamilyNet, the acting project manager for FamilyNet, and the DSS director of internal audit to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been evaluated, and whether a written business continuity plan was in place. We reviewed the written business continuity plan for appropriate content, strategic objectives, and clarity of directives and procedures. In addition, to determine whether controls were adequate to ensure that data files and software for FamilyNet and business applications would be available should the automated system be rendered inoperable, we interviewed DSS management responsible for creating backup copies of computer-related media. Further, we reviewed the adequacy of provisions for on-site and off-site storage of critical and important backup tapes. We reviewed and evaluated the adequacy of physical security and environmental protection controls for the on-site storage locations. We determined whether the FamilyNet database was being backed up nightly by storage location.

To evaluate user satisfaction regarding certain functions of FamilyNet, we selected for interview a judgmental sample of managers, caseworkers, and administrative staff from persons who were located at the central office and each regional and area office we visited. We then interviewed 56 managers and staff, including regional administrative managers, area administrative managers, program managers, casework supervisors, caseworkers, and legal personnel. Subsequently, we assessed the results of the interviews noted above to ascertain the levels of user satisfaction.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted industry control practices and auditing standards.

AUDIT SUMMARY

Based on our audit, adequate security controls were found to be in place and in effect to provide reasonable assurance that only authorized parties could access the Department of Social Services' (DSS) FamilyNet system and IT resources. Our audit indicated that, although important controls were in place to provide reasonable assurance that system information was sufficiently protected against unauthorized disclosure, change, or deletion, certain controls regarding system access to the FamilyNet system and security over hardcopy confidential records needed to be strengthened. Further, we found that DSS had implemented adequate physical security controls to provide reasonable assurance that only authorized persons could access business offices, computer rooms, and automated systems at the central office in Boston, six regional offices, and the nine area offices we reviewed. We found that, except for six computer rooms housing computer file servers, appropriate environmental protection controls were in place to prevent damage to or loss of IT-related assets.

We determined that DSS had implemented adequate business continuity plans to restore normal business functions should the automated systems be unavailable for an extended period. According to DSS management, adequate controls were in place to ensure that the nightly backup of the FamilyNet application and data files was being performed at the Massachusetts Information Technology Center (MITC). Further, we found that, except for three on-site storage locations, adequate controls were in place over backup copies of administrative applications, such as those used for word processing applications and documents at DSS offices.

With respect to data security, our audit indicated that DSS had developed a well-defined and documented policy and associated procedures regarding the protection of confidential data from unauthorized disclosure and use. In conjunction with the review of the data security policy, we found that confidential automated data was being maintained in a logical manner, inasmuch as the FamilyNet-related data dictionary was found to be appropriate and consistent. In that regard, we noted that the data dictionary used specific standard naming conventions to create a repository of names for each data element, its description, and its operational function within the information system.

Regarding system access security, our audit revealed that the processes for granting and recording authorization and activating user access privileges were appropriate. To reinforce user responsibilities regarding the protection and non-disclosure of their passwords, we recommend that DSS include within their documented control practices the requirement that users sign a formal security statement regarding the protection and appropriate use of passwords.

Although appropriate procedures were in place for authorization and activation, increased effort was needed to provide a high level of assurance that access privileges no longer needed or authorized would be deactivated in a timely manner. We determined that there was no formal mechanism in place to ensure that logon IDs and passwords would be revoked for individuals no longer authorized or needing access to automated systems, especially FamilyNet. Based on a comparison of active user privileges to the current official personnel list, we determined that 14 (14.4%) of the 97 user accounts selected were active for individuals who no longer worked for or were contracted with the Department. As of the test date, we determined that one account was active for a staff member who had not been employed with the department for 36 months. Further, we found that six other individuals had terminated employment or their contracted relationship during 1998 and 1999 and seven users had terminated employment or their contracted relationship during 2000. It was noted that four of the 14 active users had limited access to the FamilyNet system due to their contracted relationship with DSS or held positions as interns. After bringing this issue to the attention of DSS management, it is our understanding that access privileges were deactivated for users who were no longer authorized to access FamilyNet.

We recommend that DSS document and implement procedures to ensure that the security administrator is notified in a timely manner of changes in employee job status, such as terminations, transfers, or extended leaves of absence. Once notified, the system administrator should deactivate and/or delete the logon ID and password. We also recommend that the internal control plan address security violations, monitoring and reporting of access attempts, and follow-up procedures for access security violations and violation attempts. Subsequent to the close of our audit, the DSS documented control procedures regarding authorization, activation, and deactivation of access privileges for inclusion in its internal control plan.

With respect to the safeguarding of confidential client records that are in hardcopy form, we found that, except for certain control procedures at four DSS offices, adequate controls practices were in place to properly secure client records at the central office, regional offices, and five of the nine area offices reviewed during our audit. Further, we determined that sufficient documented practices were in place regarding security over client records removed for review from case-record rooms. Adequate controls, including documented practices, were in place to provide reasonable assurance that when appropriate, confidential records in hardcopy form would be properly destroyed through the use of shredding machines at DSS offices and/or removed for disposal by contracted shredding and disposal companies.

With respect to the offices visited, we determined that adequate physical security controls were in place and in effect to prevent unauthorized access, loss or disclosure of hardcopy confidential client records stored at the central office and area offices. We found that physical security controls needed to be strengthened at the Plymouth area office and the Brockton Regional and Southeast Divisional and Southeast Counsel Offices. We note that the central office in Boston would benefit from strengthening certain physical controls. Our audit disclosed that, although the Plymouth area office was maintaining client records in a locked room, the records were not consistently returned to the secure case-record room at the close of each workday. Instead, client records were placed on bookshelves, on top of or adjacent to desks, or kept in unlocked file cabinets. Further, our audit revealed that, although the case-record room at the Brockton Regional and Southeast Divisional Counsel Offices was locked, the room could be accessed from an adjacent unsecured conference room. At the central office, we found that certain file cabinets were not locked and were sometimes left unattended during normal business hours. Further, according to DSS management, these particular file cabinets were not locked after normal business hours. We also determined that the legal office within the Arlington regional office was not locked after regular business hours. Although generally a reasonable level of security was found to be in place over the offices visited during the audit, rooms or cabinets containing confidential records should be locked to afford an additional margin of security to reduce the risk of unauthorized access or unauthorized disclosure of hardcopy client records.

All information regarding clients that is entered into FamilyNet or documented in paper records is deemed by DSS under legal guidance to be confidential. In this regard, potential disclosure of client-related information to unauthorized staff or other persons may jeopardize client privacy rights and imperil their physical and/or emotional well-being. We recommend that all case records be returned to a secure location and locked in file cabinets when not in use or at the end of each workday. In addition, we recommend that management monitor work areas to help ensure that client records are not left unattended on desks or in easily accessible areas within business offices. Client records should be stored in secure rooms that can only be accessed with keys or other access control devices. Further, DSS should ensure that all staff members comply with the Department's written control practices regarding the sign-out and sign-in of client records.

We determined that the DSS offices followed appropriate procedures regarding the removal and destruction of client records no longer needed. With respect to the automated FamilyNet system, and hardcopy records, we recommend that the Department's formal policies and procedures be revised to include guidelines promulgated by the Records Conservation Board regarding retention and disposal of client records.

Our audit revealed that DSS had implemented appropriate physical security controls over the IT systems on which the FamilyNet application resides at the DSS offices we reviewed. We found that adequate controls, including key management (e.g., control practices regarding issuance and return of keys) for entrances to business offices, rooms housing file servers, and case record rooms; the presence of a receptionist; and intrusion detection devices were in place to prevent and detect unauthorized access to IT-related assets. However, our audit indicated that rooms housing file servers at the central office and the Springfield and Worcester area offices were not consistently locked. We recommend that DSS ensure that file server rooms be appropriately and consistently secured.

We determined that adequate environmental protection controls, such as documented fire emergency plans and procedures, fire detection and suppression systems, including sprinklers and inert-gas fire-suppression systems and general housekeeping practices were in place to protect personnel from physical harm and IT-related assets from loss or damage. Further, our audit indicated that controls to provide electrical power spike and surge protection, such as electrical circuit breakers, surge protectors for automated systems, and emergency power generators and lighting were in place at the DSS offices we reviewed. We found that proper temperature controls were in place at business offices, computer rooms, and on-site computer media storage areas. Control practices were also in place to help prevent water damage to automated systems, client records, and computer-related backup media. However, we noted that temperature controls in six computer rooms housing file servers needed to be improved by better monitoring and control of temperature levels.

We found that adequate controls were in effect to provide reasonable assurance that mission-critical and essential functions could be resumed in a timely manner should automated systems become inoperable or otherwise unavailable for an extended period. Our audit revealed that DSS was maintaining a current, documented, and tested business continuity plan, including manual procedures to provide continuous services to the public and clients. According to DSS management, FamilyNet-related data files and software were backed up nightly at a secure state facility operated by the Commonwealth's Information Technology Division (ITD). Our audit disclosed that, although adequate controls were in place over on-site storage of administrative applications and data at five regional and/or area offices, certain control practices at five additional sites needed to be strengthened. We determined that backup tapes were stored in unlocked rooms housing file servers at three sites, and certain tapes were not stored in fire-proof boxes at two additional area offices. We recommend that backup copies of administrative applications and data files be stored in a physically secure location, preferably in a fireproof safe or box in accordance with standards as established for computer facilities by the National Fire Protection Association. Appendix A of this report provides a summary of physical security and environmental protection controls at the DSS offices that were selected for review.

Based on survey responses from a judgmental sampling of managers and staff who were interviewed between June 22 and August 15, 2000, we concluded that the majority of DSS employees surveyed found FamilyNet to be readily available; and that the system produced accurate, complete, timely, and useful management reports for monitoring cases; and was an improvement over the prior mainframe-based system. Further, the DSS employees surveyed indicated that FamilyNet was easier to use than the prior application system, client records were easier to access and read, and client information was usually more current and detailed. Regarding the overall availability of the FamilyNet system, a significant number of DSS employees indicated that the system was usually available for use. Those surveyed also indicated that the "help desk" was available to answer questions and resolve problems; and that problems were resolved in a timely manner. However, results of the user satisfaction survey also indicated that certain staff members noted that specific system functions were in need of improvement. One frequently cited shortcoming was that, contrary to the desires of the staff, FamilyNet could only be accessed from DSS offices and not from on-site field locations. Further, respondents indicated that movement from one computer screen through multiple screens to the next was often too slow. Suggested improvements from those surveyed included restructuring certain forms, such as the service plan and risk assessment matrix, to make them more useable; developing an automated search function of with respect to client addresses; and developing access to other related statewide databases. We recommend that DSS management assess and appropriately address employee concerns as noted in the results of the user satisfaction survey. Appendix B of this report provides a summary of selected responses to the user satisfaction survey.

AUDIT RESULTS

1. System Access Security

Our audit disclosed that although certain system access security controls were in place, other control procedures needed to be strengthened to ensure that only authorized users have access to the FamilyNet system. We determined that control procedures authorizing users to access the FamilyNet system were appropriate. Those procedures included having the Human Resources Department notify both the Staffing Analysis Unit and the regional office of a newly-hired staff member. The authorization level of a new employee is based upon pre-determined levels of access assigned to the job title and associated responsibilities as designated by the Staffing Analysis Unit. Upon notification by the Staffing Analysis Unit, the Information Technology Unit activates the authorized levels of system access for each new employee. Although we found that these procedures provided an adequate authorization and activation process, we determined that DSS was not requiring users who were granted access to the Department's automated systems to sign a formal security statement acknowledging that they understood their responsibilities regarding the protection and appropriate use of their passwords. In addition, at the date of our audit, we determined that control procedures regarding authorization and activation of user access privileges were not documented or referenced in the Department's internal control plan.

We determined that control procedures regarding logon ID and password administration were documented and addressed password formation and use, periodic changes of passwords, and confidentiality requirements of passwords. Subsequent to being granted access privileges, users are assigned a unique logon ID and are required to choose a password of sufficient length and composition. To gain access to the system, the user is required to enter his/her logon ID and password. Access to system-based resources is obtained based upon the information regarding job title and responsibilities entered into the access control table.

At the time of our audit, we found that users were not changing their passwords in a timely manner. Based on Information Technology Division (ITD) requirements, DSS had strengthened control practices regarding logon ID and passwords and had implemented procedures to require more frequent password changes. According to DSS management, controls are in place within the automated system to track all accesses and access attempts to data files. Furthermore, system controls enable users to monitor normal activity within their accounts and to detect access attempts or unusual activity in their accounts in a timely manner.

With respect to procedures to deactivate access privileges, our audit revealed that adequate controls were not in place to provide reasonable assurance that access privileges would be deactivated for users no longer authorized or needing access to the automated systems. We found that, as a result, a number of logon IDs and passwords were left active for individuals no longer authorized or needing access to the system. Failure to deactivate logon IDs and passwords may allow unauthorized access to confidential client information, because the access privileges of staff who have terminated or transferred employment, or taken new positions within the Department, may continue to be available for use. Changes in employment status that should affect system access privileges are: termination of employment, change of position or job responsibilities that impact the level of access required, and extended leaves of absence when access is not required.

During the audit, we tested the DSS FamilyNet user database for the presence of unauthorized users whose access privileges remained active after the users were no longer authorized to have access. We chose a statistical sample of 97 active logon IDs for DSS employees and outsourced staff. Based on our comparison of active user privileges to the current official personnel list, we determined that 14 (14.4%) of the 97 user accounts selected were active for individuals who no longer work for or were contracted with the Department. As of the test date, we determined that one account was active for a staff member who had not been employed with the department for 36 months. Further, we found that six other individuals had terminated employment or their contracted relationship during 1998 and 1999 and seven users had terminated employment or their contracted relationship during 2000. It was noted that four of the 14 active users had limited access to the FamilyNet system due to their contracted relationship with DSS or held positions as interns. After bringing this issue to the attention of DSS management, it is our understanding that access privileges were deactivated for users no longer authorized to access FamilyNet.

We determined that DSS had not developed department-wide policies and procedures regarding notification to security administrators upon a change in employee job status that would require modification or deactivation of the users' access privileges. However, we noted that the Worcester and Attleboro/Taunton regional and area offices had developed written documentation regarding termination procedures for use by their office staff. We found that, subsequent to our audit, DSS management had documented practices regarding activation and deactivation and deletion of access privileges for staff no longer authorized to access automated systems, including FamilyNet. According to DSS administrators, the Department planned to include the control practices regarding activation, deactivation and deletion of logon IDs and passwords in the Department's internal control plan.

Generally accepted computer industry standards indicate the need to prevent unauthorized system access through the implementation of formal control procedures. Sufficient security controls should be exercised to protect the confidentiality and integrity of important and sensitive data and to limit access to data and system functions to only authorized parties. Control practices should include formal procedures to deactivate logon IDs and passwords when employee status changes. Failure to implement adequate controls regarding system access security could result in unauthorized system access or use. If unauthorized access were gained to the FamilyNet-related data files residing on the LANs' file servers or the microcomputer systems, there is risk of unauthorized disclosure, modification or deletion of critical and important data, such as confidential information regarding DSS clients.

Recommendation:

We recommend that to reinforce user responsibilities regarding access privileges, the DSS should require users to sign a formal statement acknowledging the confidentiality of their password and commitment to protect the password from unauthorized use and/or disclosure. Further, we recommend that documented practices regarding authorization and activation of access privileges be included in the Department's internal control plan. Policies and procedures should also include procedures for deactivation and deletion of logon IDs and passwords. We also recommend that DSS implement policies and procedures to help ensure that the security administrator is notified in a timely manner of changes in employee status, such as terminations, extended leaves of absence, employee transfers, and inter-departmental changes in authorization levels. Once notified of the change in employment status, the FamilyNet security administrator should deactivate and/or delete the logon ID and password in a timely manner. Appropriate staff should be instructed regarding carrying out and adherence to policies and procedures.

We recommend that DSS consider modifications to the automated system so that access privileges would be deactivated after a period of inactivity. We recommend that DSS monitor the appropriateness of users assigned access to the automated systems, and deactivate logon IDs and passwords for users no longer needing access to the system. We also recommend that the internal control plan address security violations, monitoring and reporting of access attempts, and follow-up procedures for violations and violation attempts.

Auditee's Response:

> *The Department of Social Services recognizes the importance of the issues referenced in Report Recommendations regarding System Access Security. As a result of the recommendations presented, the Department will be developing a formal document for signature by new employees during the hiring process that advises the employee(s) of the importance of maintaining the confidentiality of their assigned system(s) log-in(s) and passwords. The signed document will become a part of their employee folder.*
>
> *Further, the Department's Information Technology Unit and the Office of Human Resources is developing a procedure for the routine review of system users and Department employees to update user access records based on functional assignment changes, changes in employment status and inactivity of use. Additionally, procedures are being developed to review and update access to systems by contract and contracted provider agency personnel who*

> *utilize Department systems in the course of the assignments in support of Departmental operations and service provision.*
>
> *When the various drafted policies and procedures, associated with the report recommendations for Systems Access Security are finalized, they will be included in the Department's updated Internal Control Plan.*

Auditor's Reply:

We agree with the efforts of DSS management to improve system access security by requiring staff to sign a formal security statement regarding the non-disclosure of passwords and the protection of confidential client information. Further, we are pleased that the Department is developing control practices for the regular review of system users' access privileges. We agree with the Department's effort to develop additional internal control policies and procedures regarding authorization, activation, and deactivation of user accounts and the proper use of IT-related resources, including e-mail, data confidentiality, and appropriate use of passwords. We are pleased that the policies and procedures will be included in the Department's internal control plan. We will review system access security and the updated internal control plan at our next scheduled IT audit.

2. Security over Hardcopy Client Records

Our audit revealed that, although DSS had implemented significant security controls over hardcopy client records, certain controls at the central office, Arlington regional office, Brockton Regional and Southeast Divisional Counsel Offices, and the Plymouth area office needed to be strengthened. We determined that adequate physical security controls were in place over office areas at the Plymouth area office where client records were located. However, we found that, although client records were maintained in a locked room, DSS staff did not consistently return these records to the secure case-record room at the close of each workday. According to DSS management, all information regarding clients entered into FamilyNet or documented in paper records is deemed to be confidential. Further, the DSS "Records Management Manual", dated April 1987, states that "(e)ach office should take whatever action is necessary to prevent unauthorized access of consumer records." Further, the manual states that, ". . . records should be refiled when not in use; . . . all records must be returned to the file cabinets at the end of the day; and file cabinets and file room must be locked when the office is closed."

During our inspection of the Plymouth area office, we found that, contrary to the control procedures noted above, certain client records had been placed on bookshelves, on or adjacent to staff desks, or had been left accessible in unlocked file cabinets overnight. In addition, although client records were to be stored in a secure room, some of the records were at times kept in unlocked file cabinets or were being placed on open shelves outside of the secure room. As a result, unauthorized staff, including administrative and janitorial staff, may have had access to sensitive, confidential client information, jeopardizing clients' privacy rights, and potentially their physical and emotional well-being.

Our audit indicated that physical security over client records to be archived that were stored in a case-record retention room at the Brockton Regional and Southeast Divisional Counsel Offices needed to be improved. We determined that although the case-record room at the Brockton Regional and Southeast Divisional Counsel Offices was locked, the room could be accessed from an adjacent unsecured conference room. We found that, although for the most part, adequate physical security was in place at the central office in Boston, certain file cabinets containing confidential information were not being kept locked during or after normal business hours. Unsecured rooms or file cabinets may place confidential client records at risk of theft or unauthorized disclosure. Further, we found that the legal office at the Arlington regional office was not locked during or after normal business hours.

Massachusetts General Laws (MGL), Chapter 66, Section 12, entitled "Arrangement of Records for Reference," states that "(a)ll such records shall be kept in the rooms where they are ordinarily used, and so arranged that they may be conveniently examined and referred to. When not in use, they shall be kept in the fireproof rooms, vaults or safes provided for them." MGL, Chapter 66A, Section 2, entitled "Accountability for and Protection of Records containing Personal Data," states, in part, that "(e)very holder maintaining personal data shall: a) identify one individual immediately responsible for the personal data system who shall ensure that the requirements of this chapter for preventing access to or dissemination of personal data are followed; b) inform each of its employees having any responsibility or function in the design, development, operation, or maintenance of the personal data system, or the use of any personal data contained therein, of each safeguard required by this chapter, of each rule and regulation promulgated pursuant to section three which pertains to the operation of the personal data system; c) not allow any other agency or individual not employed by the holder to have access to personal data unless such access is authorized by statute or regulations; d) take responsible precautions to protect data from dangers of fire, theft, flood, natural disaster, or other physical threat; . . . f) in the case of data held in automated personal data systems, and to the extent feasible with data held in manual personal data systems, maintain a complete record of every access to and every use of any personal data . . ."

According to DSS management at the Plymouth area office, caseworkers were maintaining records in a less than fully protected manner because it was more convenient for them to keep client records near their work area rather than to return them to the secure case-record room that is located on a different floor. Further, DSS management at the Brockton Regional and Southeast Divisional Counsel Offices indicated that confidential client records to be archived were at increased risk of unauthorized access because of the structural design of the case-record room used to store them.

Recommendation:

We recommend that DSS management and staff, but with specific reference to offices reviewed (i.e., the central office in Boston, Plymouth area office and Brockton Regional and Southeast Divisional Counsel Offices, Arlington regional office), review statutory authority and Departmental policies and procedures regarding security over client information, develop, strengthen, and/or implement control practices where needed, monitor control practices, and ensure that staff are instructed with respect to security policies and proper procedures for safeguarding client records. We recommend that all confidential case records be returned to a secure location and locked in file cabinets when not in use or, minimally, at the end of each workday. DSS should ensure that all client records are properly signed out and signed in when removed from case-record rooms for review or update and returned for secure storage. We recommend that all client records, when not in use, be stored in locked cabinets and otherwise secure rooms that can only be accessed using keys or other access-restricting devices. Further, we recommend that management perform inspections of work areas and ensure that client records are not left unattended on desks or otherwise easily accessible areas.

Auditee's Response:

> *The Department acknowledges and recognizes the importance of and its responsibility to safeguard its consumers' records from unauthorized access, theft and or damage. As referenced in the OSA report, the Department of Social Services has in place policy and practices to address consumer record access and security.*
>
> *All offices have securable record rooms available for the maintaining of consumer records when not in use and during non-business hours. Management, at all levels of the Department will continue to advise and work with staff throughout the Department, regarding policy and procedural requirements for limiting access to and safeguarding of consumer and other types of confidential files.*
>
> *The Department understands the desirability of having confidential records maintained in locking file cabinets, however its ability to do so is subject to the appropriation process for funding an equipment purchase sufficient to comply with the recommendation put forward by the Office of the State Auditor. As noted previously, the Department does maintain the ability to secure and safeguard consumer and other confidential records absent the receipt of additional locking file cabinets.*

Auditor's Reply:

We are pleased that DSS recognizes the importance of safeguarding confidential client records in hardcopy form from unauthorized access, theft, disclosure, or damage. Given the significance of securing client records in locked file cabinets and budgetary limitations, we recommend that, as an interim solution, DSS contact the Operational Services Division to determine the availability of locked file cabinets currently placed in surplus property. Should the file cabinets be unavailable, we recommend that DSS request that OSD notify the Department when locking file cabinets become available. We will review controls regarding confidential client records at our next scheduled IT audit.

While it may be difficult to exercise ideal security practices in all office areas, increased attention on the need to secure client records when they are not being used in the normal course of work will strengthen the system of internal control. We did not detect any specific instances where the level of security observed placed a client's well-being at risk. Our examination, on the other hand, indicated that in some work areas controls over client records needed to be strengthened to reduce the risk of unauthorized access or disclosure of confidential information.

Additional Auditee Responses

> *The Department wishes to note that with the exception of the lack of a sprinkler system in its Plymouth Area Office, which is regulated by applicable building code(s), many of the "Inadequate" findings have been resolved since the various site visits, made by Office of the State Auditor staff, took place.*
>
> *Notable has been the installation of additional air conditioning units in server locations that have enhanced both the environmental safety, and physical security of various systems hardware. This has resulted from a combination of additional equipment purchases and buildouts of existing or new office space locations as the result of new leases.*
>
> *The "Inadequate" notations involving office security issues including visitor sign-ins, wearing of ID badges, installation of intrusion alarms and standardization of security aspects associated with employee terminations are either currently under review or will be reviewed Department-wide, with heightened interest and priority since and following the events of September 11, 2001*
>
> *Some security enhancements now under consideration include (but are not limited to) the need for staff to wear photo ID badges in offices, further limitation of access to office spaces by preventing entrance to space by means of side and back entrances. The issuance of visitor passes at all office locations and the changing of combinations for door hardware as deemed advisable due to employee termination(s) or a regularly scheduled basis are being evaluated also. As these enhancements, policies and procedures are developed and implemented, staff will be trained and, the Department's Internal Control Plan will be appropriately updated.*

Auditor's Reply:

We are pleased that DSS has corrected, or in the process of addressing, a significant number of control deficiencies related to physical security and environmental protection. We agree with the Department's efforts to address additional physical security controls such as the use of photo ID badges by staff, the issuance of visitor passes, and the periodic change of combination locks on doors. As with any well-structured system of internal control, it is also important to incorporate appropriate procedures to ensure that management control practices are monitored and evaluated for their continued appropriateness, adequacy, and compliance with internal control directives. We also agree that the DSS internal control plan should be updated as new security procedures are implemented. We will review physical security and environmental protection controls at our next scheduled IT audit.

Appendix A

Review of Physical Security and Environmental Protection at Selected DSS Offices

Department of Social Services Offices	**Business Office Secured**	**File Server Room Secured**	**Authorized Access List of DSS Personnel**	**Visitors Sign In**	**Visitors Are Escorted**	**Visitors Wear ID Badges**	**On-Site Storage of Data Tapes Secured**
Boston Central Office	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**	**Adequate**
Boston Regional Office	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**
William E. Warren Center Area Office	**Adequate**	**N/A**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**N/A**
Arlington Regional Office	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**	**Adequate**
Arlington Area Office	**Adequate**	**N/A**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**	**N/A**
Worcester Regional Office	**Inadequate**	**N/A**	**Adequate**	**Inadequate**	**Adequate**	**Inadequate**	**N/A**
Worcester Area Office	**Adequate**	**Inadequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**
Brockton Regional Office	**Adequate**	**N/A**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**
Brockton Area Office	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**
Lawrence Regional Office	**Adequate**	**N/A**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**	**N/A**
Lawrence Area Office	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**	**Adequate**
Springfield Regional Office	**Adequate**	**N/A**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**	**N/A**
Springfield Area Office	**Adequate**	**Inadequate**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**	**Inadequate**
Plymouth Area Office	**Adequate**	**Adequate**	**Adequate**	**Inadequate**	**Adequate**	**Inadequate**	**Adequate**
Attleboro Taunton Area Office	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**
Coastal (Weymouth) Area Office	**Adequate**	**Adequate**	**Adequate**	**Inadequate**	**Adequate**	**Inadequate**	**Adequate**

Key:

Adequate = Controls in place provide reasonable level of assurance that physical security and environmental control objectives will be met.

Inadequate = Controls need to be strengthened to provide reasonable level of assurance that physical security and environmental control objectives will be met.

N/A = Not applicable.

Appendix A

Review of Physical Security and Environmental Protection at Selected DSS Offices

Offices	Intrusion Alarms	Fire Alarm	Temperature of File Server Room	Water Sprinklers	Confidential Hardcopy Information Secured Within the Business Office	Client Confidential Hardcopy Information Secured (Case Record Room)	Confidential Hardcopy Information Disposed of Properly	Office's Own Policy and Procedure for Termination of Employees
Boston Central Office	**Inadequate**	**Adequate**	**Inadequate**	**Adequate**	**Inadequate**	**N/A**	**Adequate**	**Inadequate**
Boston Regional Office	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**N/A**	**Adequate**	**Inadequate**
William E. Warren Center Area Office	**Adequate**	**Adequate**	**N/A**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**
Arlington Regional Office	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**	**N/A**	**Adequate**	**Inadequate**
Arlington Area Office	**Adequate**	**Adequate**	**N/A**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**
Worcester Regional Office	**Adequate**	**Adequate**	**N/A**	**Adequate**	**Adequate**	**N/A**	**Adequate**	**Adequate**
Worcester Area Office	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**
Brockton Regional Office	**Inadequate**	**Adequate**	**N/A**	**Adequate**	**Inadequate**	**N/A**	**Adequate**	**Inadequate**
Brockton Area Office	**Inadequate**	**Adequate**	**Inadequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**
Lawrence Regional Office	**Inadequate**	**Adequate**	**N/A**	**Adequate**	**Adequate**	**N/A**	**Adequate**	**Inadequate**
Lawrence Area Office	**Inadequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**
Springfield Regional Office	**Adequate**	**Adequate**	**N/A**	**Adequate**	**Adequate**	**N/A**	**Adequate**	**Inadequate**
Springfield Area Office	**Adequate**	**Adequate**	**Inadequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**
Plymouth Area Office	**Adequate**	**Adequate**	**Inadequate**	**Inadequate**	**Inadequate**	**Adequate**	**Adequate**	**Inadequate**
Attleboro Taunton Area Office	**Adequate**	**Adequate**	**Inadequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**
Coastal (Weymouth) Area Office	**Adequate**	**Adequate**	**Inadequate**	**Adequate**	**Adequate**	**Adequate**	**Adequate**	**Inadequate**

Key:

Adequate = Controls in place provide reasonable level of assurance that physical security and environmental control objectives will be met.

Inadequate = Controls need to be strengthened to provide reasonable level of assurance that physical security and environmental control objectives will be met.

N/A = Not applicable.

Appendix B
FamilyNet User Satisfaction Survey
Summary of Selected Responses to the User Survey Questionnaire

Interviews were conducted with a sample of 56 administrators, managers, supervisors, and social workers chosen judgmentally from DSS staff employed at six (6) Regional Offices, nine (9) Area Offices and the Boston Central Office between June and August of the calendar year 2000.

1. How do you use FamilyNet in your job?

   The most common responses were:

   - **Review reports, such as Foster Care review schedules, logs of consumers served, and caseload statistics**
   - **Approve service referrals, travel and client search and case tracking**
   - **Check status of casework through case tracking and screening reports**

2. How long have you used FamilyNet?

   - **4% 6 months to 1 year**
   - **89% 1 year to 2 years**
   - **7% More than 2 years**

3. Is FamilyNet an improvement over the prior automated system?

   - **79% Yes**
   - **8% No**
   - **13% Not applicable or did not know**

   Most commonly cited improvements were:

   - **Case "record" information much easier to read**
   - **Information more detailed, easier to use and secure**
   - **Up-to-date information**

4. What features of the system do you like best and least?

   a. Most commonly-liked features were:

   - **Easy access to case records**
   - **Case "record" much easier to find and read**
   - **Management reports make it much easier to monitor cases**

   b. Most commonly-disliked features were:

   - **FamilyNet system requires caseworkers to work in the office not the field**
   - **System response time too slow**
   - **Screen navigation process needs improvement**

Appendix B
FamilyNet User Satisfaction Survey
Summary of Selected Responses to the User Survey Questionnaire

5. What features would you like to see changed?

Selected responses included:

- **Increase speed of FamilyNet response time**
- **Forms such as service plans and risk assessment matrix are cumbersome to use**
- **FamilyNet resources and adoption modules need improvement**
- **Need improved client address search**
- **Access to related statewide databases**
- **Streamline reports**

6a. What type of training have you received regarding use of the system?

- **Basic FamilyNet training for assigned duties and responsibilities**
- **Training on use of specific screen**

6b. Has the training been adequate?

- 80**% Yes**
- **17% No**
- **3% Not Applicable or Did Not Know**

6c. When was the last date of training?

- **75% Within the Last 6 months**
- **9% 6 months to 1 year**
- **10% 1 year to 2 years**
- **6% More than 2 years ago**

6d. What suggestions would you have to improve the training?

- **Continuous training at the central office and more on-site training**
- **Ongoing training for the caseworkers**
- **Conduct training with a hardcopy manual**

7. Are you aware of a "help desk" available to answer questions and resolve problems?

- **86% Yes**
- **3% No**
- **11% Not Applicable or Did Not Know**

Appendix B
FamilyNet User Satisfaction Survey
Summary of Selected Responses to the User Survey Questionnaire

8. Have questions regarding use of the system and reported problems been resolved in a timely manner?

- **82% Yes**
- **11% No**
- **7% Not Applicable or Did Not Know**

9. The system is available:

- **91% Most of the time**
- **9% Some of the time**

10a. What reports do you receive?

Common responses included:

- **Regional managers: compliance, visitation, and children in care and caseload reports**
- **Area administrative managers: loss of consumer and compliance reports**
- **Supervisors: statistics, expiring voluntary placements, parent/child visits, assessments, and service plan report**
- **Caseworkers: updates on enhancements**

10b. Are the reports timely?

- **68% Yes**
- **18% No**
- **14% Not Applicable or Did Not Know**

10c. Is the information in the reports always accurate and complete?

- **75% Yes**
- **11% No**
- **14% Not Applicable or Did Not Know**

11. Is the information useful in your work?

- **70% Yes**
- **12% No**
- **18% Non Applicable or Did Not Know**

Appendix B
FamilyNet User Satisfaction Survey
Summary of Selected Responses to the User Survey Questionnaire

12. Reports provide:

Required levels of detail:

- **57% Yes**
- **18% No**
- **25% Non Applicable or Did Not Know**

Required levels of summary:

- **59% Yes**
- **5% No**
- **36% Not Applicable or Did Not Know**

13. If the reports were not useful, what reports or additional information would be helpful?

Responses by job category included:

<u>Manager</u>

- **Additional information by town, type of cases, daily caseload summary, budget information, more foster home information, and residential programs**
- **Information categorized by area office and reports categorized by unit or worker**

<u>Supervisor</u>

- **Reports that summarize information from staff**
- **Office directory of staff**

<u>Caseworker</u>

- **Ability to locate records by case names as well as numbers**
- **Visitation reports: reason why visits did not happen**

<u>Legal</u>

- **A report of each attorney telling us how many cases he/she has without having each case and giving voluminous information about each case**
- **One report by area office showing all permanency hearings**

Appendix B
FamilyNet User Satisfaction Survey
Summary of Responses to the User Survey Questionnaire

14. The quality and readability of output media (screens or reports) are:

- **16% Excellent**
- **67% Good**
- **13% Fair**
- **4% Poor**

15. What are your major concerns for processing data in the event that the FamilyNet system was unavailable for an extended period of time?

No major concerns were cited because intake procedures and other casework could be performed manually or information could be entered via microcomputer onto disk.

16. Has the system been unavailable for an extended period?

- **77% Yes**
- **23% No**

17. Are you aware of a backup plan for FamilyNet?

- **41% Yes**
- **55% No**
- **4% Not Applicable or Did Not Know**

18. Have you been trained in a backup plan?

- **41% Yes**
- **55% No**
- **4% Not Applicable or Did Not Know**

19. Are user manuals (e.g., hardcopy and/or on-line) available to you?

- **84% Yes**
- **11% No**
- **5% Not Applicable or Did Not Know**

20. Are the user manuals helpful in performing your work?

- **88% Yes**
- **7% No**
- **5% Non Applicable or Did Not Know**

Appendix B
Family Net User Satisfaction Survey
Summary of Responses to the User Survey Questionnaire

21. Is the on-line documentation helpful?

80%	**Yes**
4%	**No**
16%	**Not Applicable or Did Not Know**